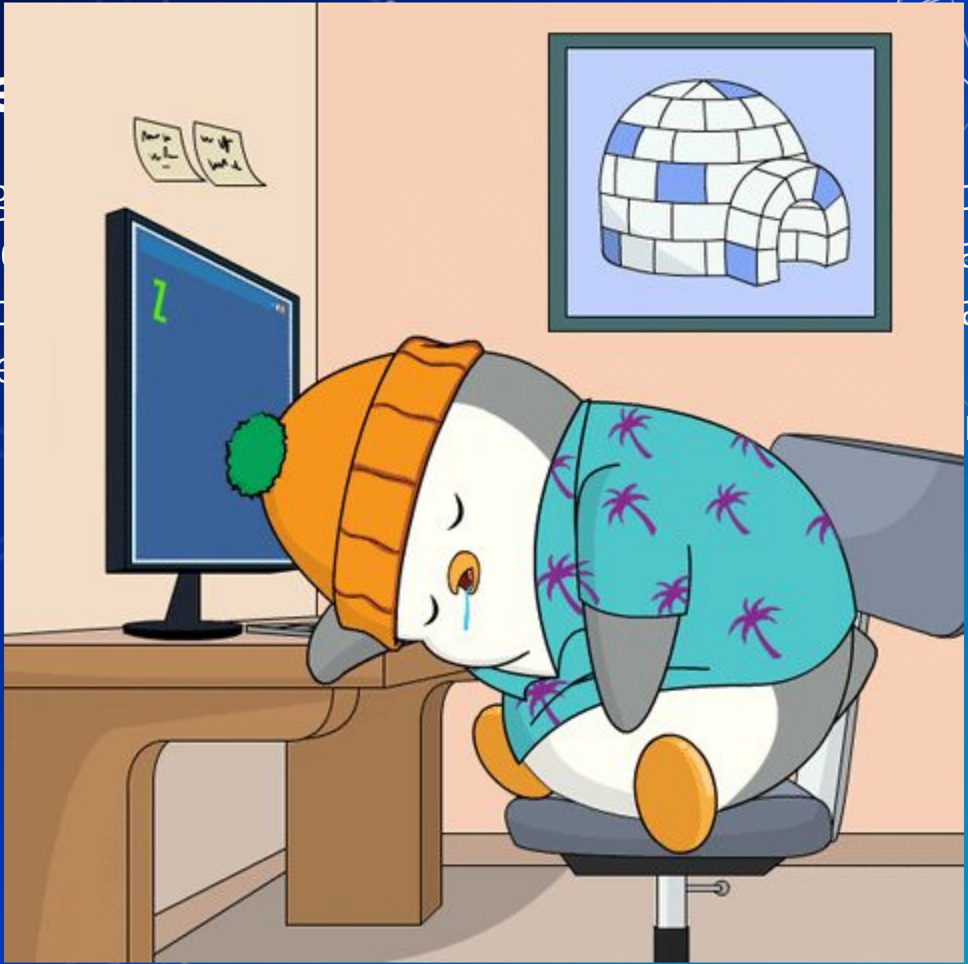
Pentesting

What is pentesting?

Penetration Testing, also colloquially known as "pen testing," is a cybersecurity practice where a group of professionals, acting as malicious actors, attempt to find, identify, and exploit vulnerabilities in a computer system. This simulated attack is supervised and carefully documented with the end goal of determining business risk towards a particular system and to help organizations understand their security posture.

What is pente

Penetration Testing persecurity
practice where a gr attempt to find,
identify, and exploit ated attack is
supervised and care ing business
risk towards a parti nd their
security posture.



What is pentesting?

- Goal: Identify security weaknesses before they are exploited by real attackers.
- Security audit testing to find and exploit vulnerabilities in a target.
- “Find security weakness before the bad guys do”
- Is <insert security control> actually implemented?
    - Is it implemented the way it should be?

Types of Pentesting

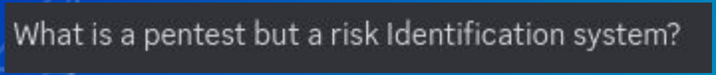
- Boot2root challenges
  - Pentesting challenges where the goal is to get root (or SYSTEM) level access.
- Web Apps
  - Discord, CRMS, your CSE442 Project.
- Hardware
  - PCB and Embedded Systems
- Systems
  - Industrial Control Systems
  - Mobile - Phones

Types of Pentesting

- Black Box
  - Done without the internal knowledge of the products.
  - See also: Functional testing.
- Grey Box
  - Some minimal information is known about the target.
  - Often used with Webapps.
- White Box
  - Full details of system are known ahead of time.

Reporting

- Remember that reporting in week 11 for risk?
- It’s back.
- Reporting is a critical part of pentesting.
  - Want to record how vulnerabilities were found and exploited.
- Many tools to integrate into your workflow.
  - I like casenotes.py



What is a pentest but a risk Identification system?

Before You Begin

A brief thought experiment.

Before You Begin

18 U.S.C 1030: Computer Fraud And Abuse Act

Something you really don’t want to mess with. [1] [2] [3] [4]

Before You Begin

18 U.S.C 1030: Computer Fraud And Abuse Act

Something you really don’t want to mess with. [1] [2] [3] [4]

FBI CYBER DIVISION

IDENTIFY • PURSUE • DEFEAT

Before You Begin

18 U.S.C 1030: Computer Fraud And Abuse Act

Something you really don’t want to mess with. [1] [2] [3] [4]

Don’t do anything you learn here on a system you don’t have express permission to do it on.

Federal Prison is bad!

Frameworks

- Lockheed Martin Cyber Kill Chain (CKC)
- MITRE ATT&CK
- PTES
  - PTF
- OSSTMM
- NIST CSF
- NCSC CAF
- (Many domain specific ones: MSTG, FSTM)
- Metasploit/Cobalt Strike*

Countless frameworks exist. You don’t need to commit yourself to one. They just serve to structure and outline an approach.

Different domains will have different requirements. Many frameworks share the same “core” features.

Frameworks

- Metasploit is a comprehensive security assessment and penetration testing framework that can automate a lot of pentesting and exploitation development.

- While very powerful, this lecture will not heavily focus on it.
- This lecture is aimed more towards the base techniques.
  - If you understand these you can pick up metasploit super easily.

- Further reading:
- https://www.offsec.com/metasploit-unleashed/
- https://www.rapid7.com/db/

Stage 0: Pre Engagement

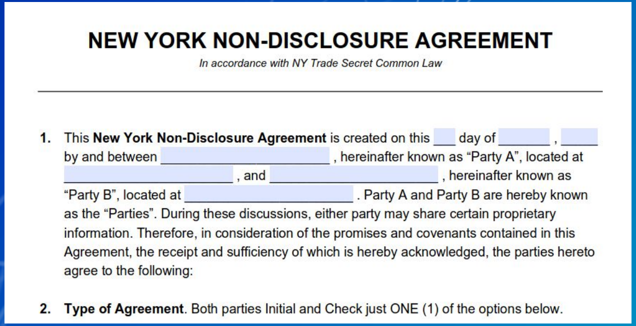
- Define Scope
  - If you have to think about something can be touched, it most likely is not in scope
- Identify Stakeholders
- Set Rules of Engagement (RoE)
- Agree on Legal and Ethical Considerations
- Establish Communication Channels
- Determine the Budget and Timeline

Stage 0: Pre Engagement

Non Disclosure Agreements

A legal contract or part of a contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to.

An NDA binds a person who has signed it and prevents them from discussing any information included in the contract with anyone not authorized by the NDA. NDAs are commonly used to protect trade secrets, business negotiations, and client information.



NEW YORK NON-DISCLOSURE AGREEMENT

In accordance with NY Trade Secret Common Law

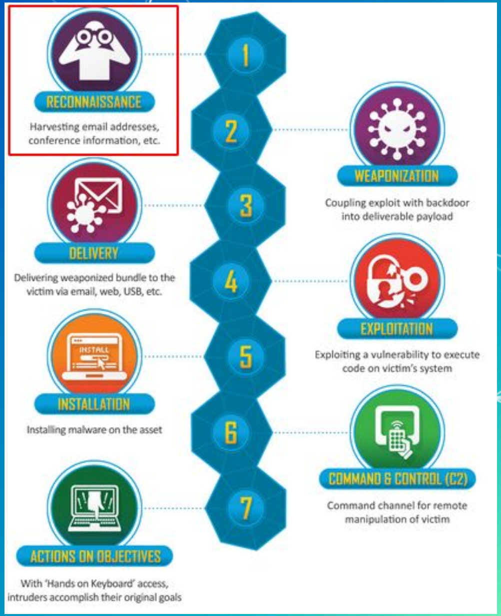
1. This **New York Non-Disclosure Agreement** is created on this ___ day of ________ , ______ by and between __________________________ , hereinafter known as "Party A", located at __________________________ , and __________________________ , hereinafter known as "Party B", located at __________________________ . Party A and Party B are hereby known as the "Parties". During these discussions, either party may share certain proprietary information. Therefore, in consideration of the promises and covenants contained in this Agreement, the receipt and sufficiency of which is hereby acknowledged, the parties hereto agree to the following:

2. **Type of Agreement**. Both parties Initial and Check just ONE (1) of the options below.

Stage 1: Reconnaissance

- "Attacker Research"
- The attacker gathers information on the target before the actual attack starts
- 2 Main Categories:
  - Active
  - Passive

Step 1 in every single framework ever mentioned.



RECONNAISSANCE

Harvesting email addresses, conference information, etc.

WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

INSTALLATION

Installing malware on the asset

COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

ACTIONS ON OBJECTIVES

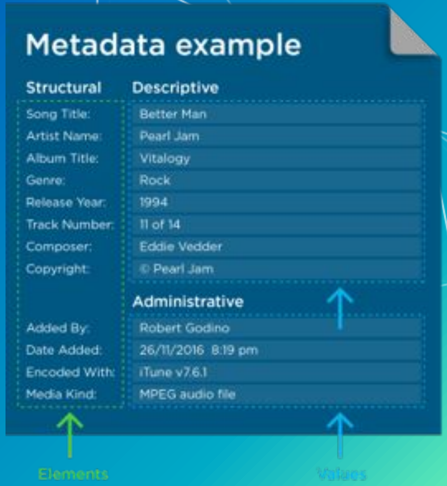
With 'Hands on Keyboard' access, intruders accomplish their original goals

Stage 1: Reconnaissance

- Passive Reconnaissance
  - Without directly interacting with the target.
  - Interaction: Network traffic between two party.
- Open Source Intelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context.
- More on this in week 15.

Types of Information you can find

- Physical (Google Maps Street View)
- Human Resources - Org Chart (Google)
- Metadata
- Infrastructure Asset
    - Network block, Subdomains, Tech stacks, Applications
- Financial
- Archives - Wayback machine
- Employees (Linkedin)
- Code (GitHub)



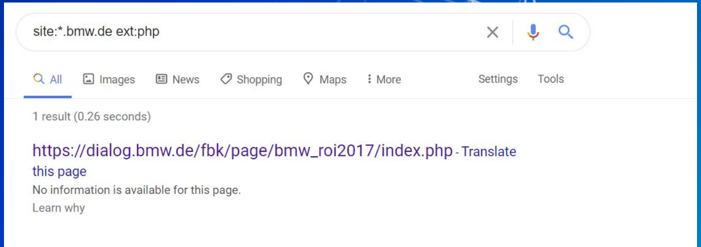
Metadata example

Structural	Descriptive
Song Title:	Better Man
Artist Name:	Pearl Jam
Album Title:	Vitalogy
Genre:	Rock
Release Year:	1994
Track Number:	11 of 14
Composer:	Eddie Vedder
Copyright:	© Pearl Jam
	Administrative
Added By:	Robert Godino
Date Added:	26/11/2016 8:19 pm
Encoded With:	iTune v7.6.1
Media Kind:	MPEG audio file

Elements
Values

Google Dorking

- Using Google's (or any other search engine) indexing capability to find information that isn't available at first glance.
- Example Dorks: mail/u/0 filetype:pdf, site:*.domain.tld ext:txt
- Useful Sites:
  - https://www.exploit-db.com/google-hacking-database



site:*.bmw.de ext:php

1 result (0.26 seconds)

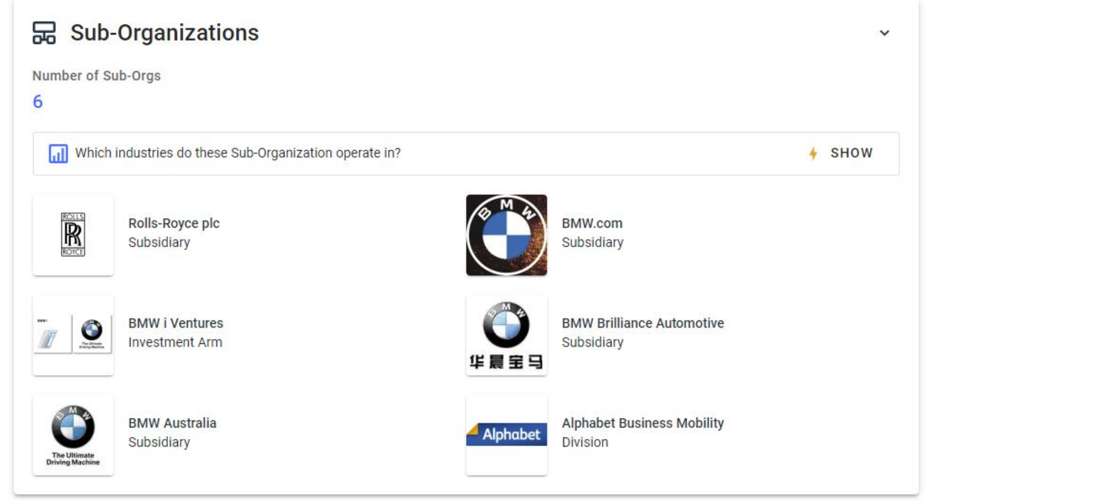
https://dialog.bmw.de/fbk/page/bmw_roi2017/index.php - Translate this page

No information is available for this page.

Learn why

Locating Subsidiaries

- When conducting a large scale penetration test identifying subsidiaries allows for a significantly larger attack surface
  - Useful Sites:
  - https://www.crunchbase.com/organization/companyName



Sub-Organizations

Number of Sub-Orgs

6

Which industries do these Sub-Organization operate in? SHOW

Rolls-Royce plc
Subsidiary

BMW.com
Subsidiary

BMW i Ventures
Investment Arm

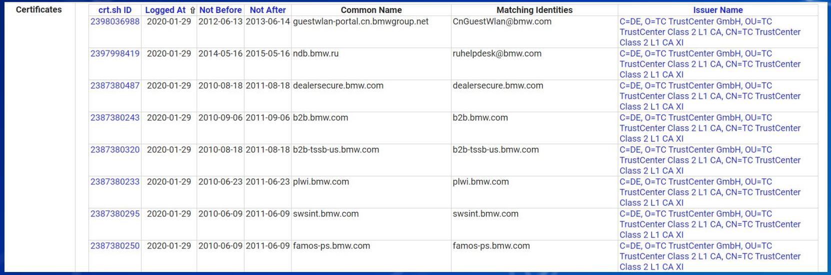
BMW Brilliance Automotive
Subsidiary

BMW Australia
Subsidiary

Alphabet Business Mobility
Division

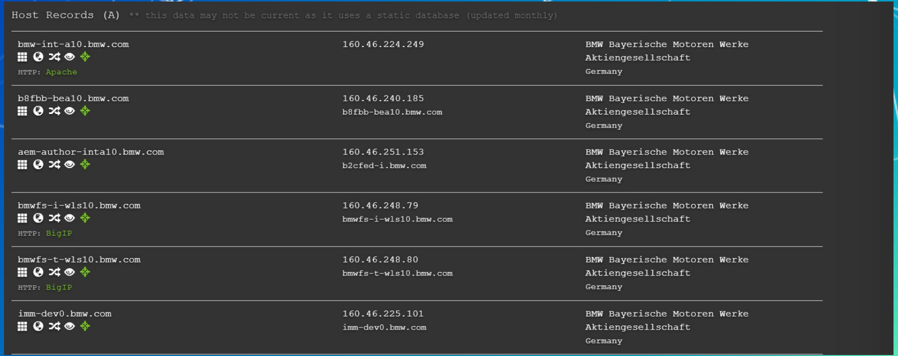
Finding Subdomains

- Subdomain - simply a domain that is a part of another domain
  - Examples: mail.google.com, cse.buffalo.edu, public.compute.thevasu.xyz
- Often host unique (and possibly vulnerable) services
- Useful Sites:
  - https://talosintelligence.com/
  - https://dnsdumpster.com/
  - https://crt.sh/?q=domain.tld



Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
2398036988	2020-01-29	2012-06-13	2013-06-14	guestwlan-portal.cn.bmwgroup.net	CnGuestWlan@bmw.com	C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Class 2 L1 CA, CN=TC TrustCenter Class 2 L1 CA XI
2397998419	2020-01-29	2014-05-16	2015-05-16	ndb.bmw.ru	ruhelpdesk@bmw.com	C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Class 2 L1 CA, CN=TC TrustCenter Class 2 L1 CA XI
2387380487	2020-01-29	2010-08-18	2011-08-18	dealersecure.bmw.com	dealersecure.bmw.com	C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Class 2 L1 CA, CN=TC TrustCenter Class 2 L1 CA XI
2387380243	2020-01-29	2010-09-06	2011-09-06	b2b.bmw.com	b2b.bmw.com	C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Class 2 L1 CA, CN=TC TrustCenter Class 2 L1 CA XI
2387380320	2020-01-29	2010-08-18	2011-08-18	b2b-tssb-us.bmw.com	b2b-tssb-us.bmw.com	C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Class 2 L1 CA, CN=TC TrustCenter Class 2 L1 CA XI
2387380233	2020-01-29	2010-06-23	2011-06-23	plwi.bmw.com	plwi.bmw.com	C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Class 2 L1 CA, CN=TC TrustCenter Class 2 L1 CA XI
2387380295	2020-01-29	2010-06-09	2011-06-09	swsint.bmw.com	swsint.bmw.com	C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Class 2 L1 CA, CN=TC TrustCenter Class 2 L1 CA XI
2387380250	2020-01-29	2010-06-09	2011-06-09	famos-ps.bmw.com	famos-ps.bmw.com	C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Class 2 L1 CA, CN=TC TrustCenter Class 2 L1 CA XI

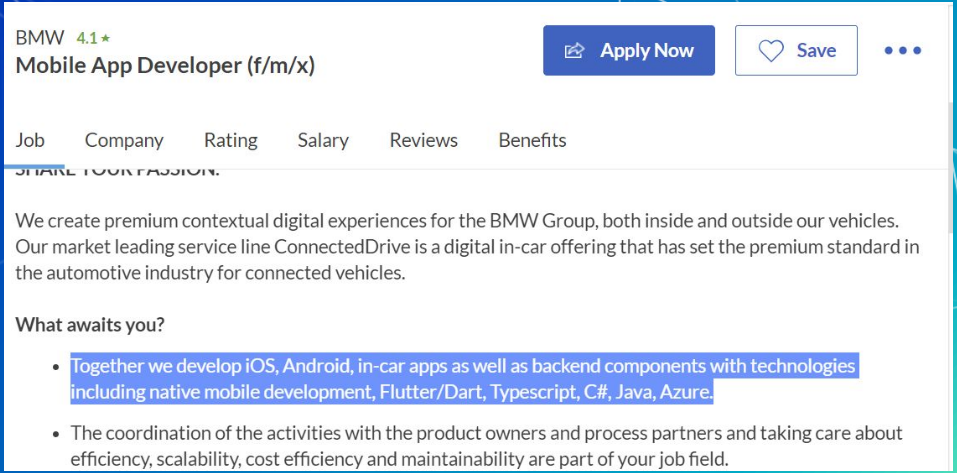


Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

bmw-int-a10.bmw.com HTTP: Apache	160.46.224.249	BMW Bayerische Motoren Werke Aktiengesellschaft Germany
b8fbb-bea10.bmw.com	160.46.240.185 b8fbb-bea10.bmw.com	BMW Bayerische Motoren Werke Aktiengesellschaft Germany
aem-author-inta10.bmw.com	160.46.251.153 b2cfed-i.bmw.com	BMW Bayerische Motoren Werke Aktiengesellschaft Germany
bmwfs-i-wls10.bmw.com HTTP: BigIP	160.46.248.79 bmwfs-i-wls10.bmw.com	BMW Bayerische Motoren Werke Aktiengesellschaft Germany
bmwfs-t-wls10.bmw.com HTTP: BigIP	160.46.248.80 bmwfs-t-wls10.bmw.com	BMW Bayerische Motoren Werke Aktiengesellschaft Germany
imm-dev0.bmw.com	160.46.225.101 imm-dev0.bmw.com	BMW Bayerische Motoren Werke Aktiengesellschaft Germany

Job Postings

- Company job listings are a great way to find what technologies the company uses
- Useful Sites:
  - https://www.linkedin.com/jobs
  - https://glassdoor.com
  - https://indeed.com



Mobile App Developer (f/m/x)

SHARE YOUR PASSION:

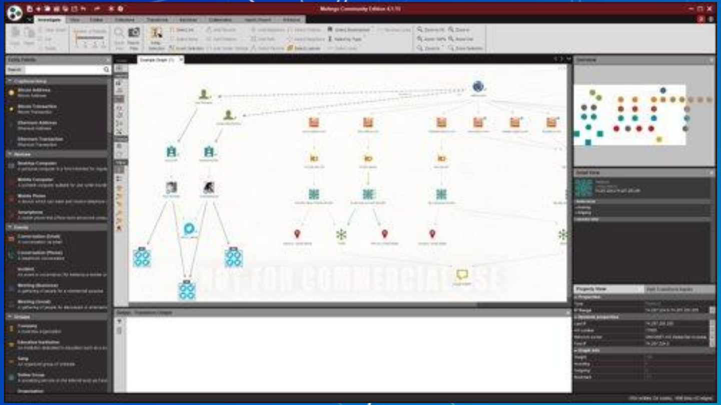
We create premium contextual digital experiences for the BMW Group, both inside and outside our vehicles. Our market leading service line ConnectedDrive is a digital in-car offering that has set the premium standard in the automotive industry for connected vehicles.

What awaits you?

- Together we develop iOS, Android, in-car apps as well as backend components with technologies including native mobile development, Flutter/Dart, Typescript, C#, Java, Azure.
- The coordination of the activities with the product owners and process partners and taking care about efficiency, scalability, cost efficiency and maintainability are part of your job field.

Passive Recon: Tools

- Frameworks
  - Osintframwork.com
  - Maltego
  - Provides big picture
  - Not the most accurate
  - Ghunt (gmail hunting)
- Search Engines
  - Google - Google dorking - (exploit-db.com/google-hacking-database)
  - DuckDuckgo
  - Baidu - China
  - Yandex - Russia
  - Nation-specific search engines
- Shodan.io
  - Scans the internet for devices and services
  - Great for asset discovery



SHODAN

Stage 1: Reconnaissance

- Active Reconnaissance
  - Enumeration performed through directly interacting with the target
  - Valid Requests
  - Malformed Requests
  - Brute Forcing
- Valid Requests
  - Loose Configuration
  - Lack of Security Awareness → "That'll be fine, np"
- Malformed Requests
  - Taking advantage of error messages
  - A LOT of Requests

Active Recon: Tools

- Nmap
- Smbclient
- Crackmapexec
- Ldapsearch
- Smbmap
- Many Many domain specific tools
  - Google them!

Nmap

```
nmap -p- -oN results.txt -sV 192.168.15.181
```

- Your best friend for network enumeration.
- `-p-` is scan for all ports
- `-oN` is output to standard text format
- -`T3` - timing template, speed! Range T0-T5 (bigger is faster)
- `-sV` - service version scan (good for enumerating services)
- `-sU` - scans UDP ports (needs root privs!)
- `-p` - scans specific port (-p- for all ports!)
- Can also specify subnets: 192.168.15.0/24

Other Common Tools

- dirbuster/gobuster
    - User for enumerating websites and directory files.
    - https://raw.githubusercontent.com/3ndG4me/KaliLists/master/dirbuster/directory-list-lowercase-2.3-small.txt
- Burp Suite
    - Web app scan and enumeration tool
- netcat
    - General purpose TCP/UDP network tool
- Sqlmap
    - Scans for SQL injections.

Step 2: Resource Development

- “Getting setup to actually attack the target”.
- Finding (or creating) exploits for know targets.
- Developing phishing campaigns.
- Can be as simple as a fake website with a malicious link
  - Or *very very* complicated.
- Creates a malicious payload to send to the target.
- Commonly some kind of trojan that can be run on target machine when dealing with humans.

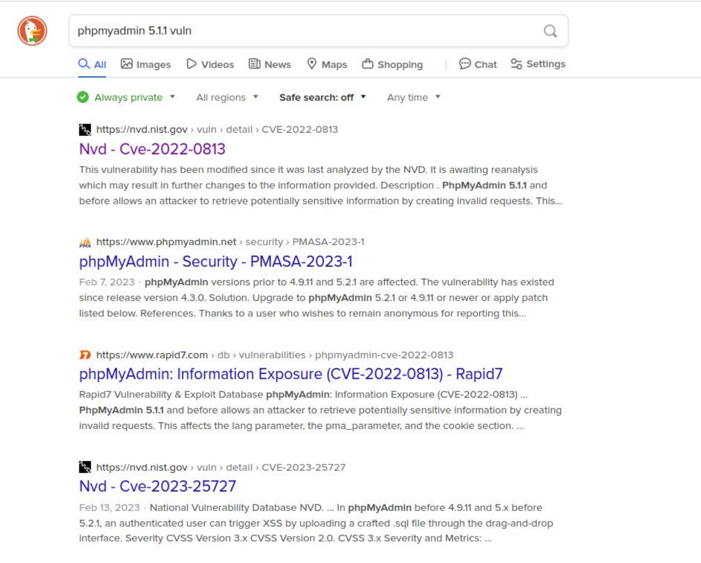
MITRE ATT&CK, CKC, PETS

What is an Exploit?

- A bug that enables an actor to compromise a system
- For our purposes; a way of gaining access to a system
- Well known exploits include:
  - Eternal Blue
  - Dirty Cow
  - Shellshock
  - Heartbleed
  - Many more...

Common things to look for

- Common Vulnerabilities and Exposures (CVE)
  - Operated by US DHS.
  - Reference method for publicly known information-security vulnerabilities and exposures.
- Backdoors
- Proof on Concept Exploits
- Develop your own!
  - Beyond the scope of this class.
- https://www.exploit-db.com/
- https://www.rapid7.com/db/



https://nvd.nist.gov › vuln › detail › CVE-2022-0813

Nvd - Cve-2022-0813

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided. Description . **PhpMyAdmin 5.1.1** and before allows an attacker to retrieve potentially sensitive information by creating invalid requests. This...

https://www.phpmyadmin.net › security › PMASA-2023-1

phpMyAdmin - Security - PMASA-2023-1

Feb 7, 2023 · **phpMyAdmin** versions prior to 4.9.11 and 5.2.1 are affected. The vulnerability has existed since release version 4.3.0. Solution. Upgrade to **phpMyAdmin** 5.2.1 or 4.9.11 or newer or apply patch listed below. References. Thanks to a user who wishes to remain anonymous for reporting this...

https://www.rapid7.com › db › vulnerabilities › phpmyadmin-cve-2022-0813

phpMyAdmin: Information Exposure (CVE-2022-0813) - Rapid7

Rapid7 Vulnerability & Exploit Database **phpMyAdmin**: Information Exposure (CVE-2022-0813) ... **PhpMyAdmin 5.1.1** and before allows an attacker to retrieve potentially sensitive information by creating invalid requests. This affects the lang parameter, the pma_parameter, and the cookie section. ...

https://nvd.nist.gov › vuln › detail › CVE-2023-25727

Nvd - Cve-2023-25727

Feb 13, 2023 · National Vulnerability Database NVD. ... In **phpMyAdmin** before 4.9.11 and 5.x before 5.2.1, an authenticated user can trigger XSS by uploading a crafted .sql file through the drag-and-drop interface. Severity CVSS Version 3.x CVSS Version 2.0. CVSS 3.x Severity and Metrics: ...

Common Mishaps and Misconfigurations

- Shared Library / Supply Chain Attacks
- File Upload
- Bad Permissions
- Server side leaking
    - Recall from Secure Coding
- Default creds
    - Very common. If you see a login page google default creds for it.

Demo

My friend Graham Edwards's company recently had some contractors build a filestore and sharing service for him. He doesn't really trust them so he asked me to see if I noticed anything about it and he'll buy me dinner next time he's in town.

The tool (called FileStorm) is located at filestorm.futuretools.us Because it's already been integrated into the rest of the infrastructure he doesn't want me to touch any other device on the network.

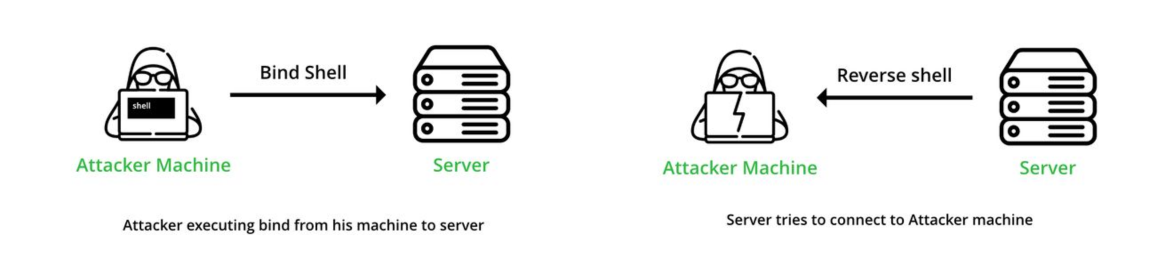
Step 3: Initial Access / Delivery

- Transmission of malware to host.
- Get some level of access to stage for later attack.
- Often results in initial lower level shell or less privileged access.
  - Sometimes not as convenient to interact with.
- 3 common vectors:
  - E-mail attachments
  - USB drives
  - Websites
- Alternatively exploit a configured vulnerability.
  - Metasploit

MITRE ATT&CK, CKC, PTES

Bind and Reverse Shells

- Bind Shells - Shells that listen on a port
  - Think SSH without a password
  - Netcat Shell
    - nc -lp 4444 -e /bin/bash
- Reverse Shells - Shells that call back to an attackers server
  - Can be created from almost any language including Bash, Python, PHP, Perl, and Ruby
  - https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md


Bind Shell
shell
Attacker Machine
Server
Attacker executing bind from his machine to server
Reverse shell
Attacker Machine
Server
Server tries to connect to Attacker machine

Demo

My friend Graham Edwards's company recently had some contractors build a filestore and sharing service for him. He doesn't really trust them so he asked me to see if I noticed anything about it and he'll buy me dinner next time he's in town.

The tool (called FileStorm) is located at filestorm.futuretools.us Because it's already been integrated into the rest of the infrastructure he doesn't want me to touch any other device on the network.

Hands On

UBNetDef is developing a multi role chatops server in preparation for an upcoming competition. The only problem was that some of the developers ran out of redbull half way through the project so it's probably not secure as it should be.

They've asked you to use your skills from the Pentesting lecture to identify and exploit **at least one** method of gaining initial access to the system.

The system is located at ??? on your ServerNet network.

Defensive Evasion

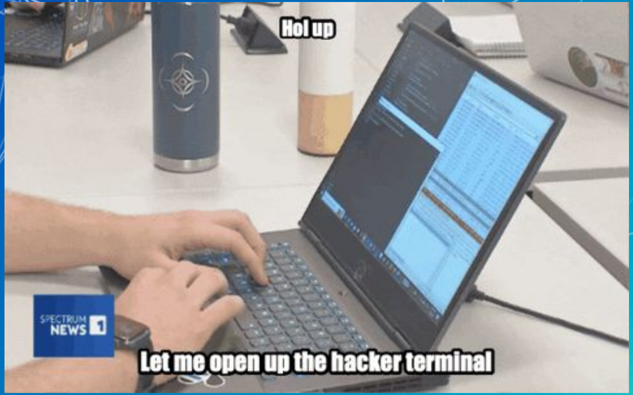
- Techniques used to avoid detection throughout their compromise.
  - Host based vs Network based.
- Uninstalling/disabling security software.
- Obfuscating/encrypting data and scripts.
- Abusing trusted processes to hide and masquerade their malware.

Putting this into practice is largely beyond the scope of this lecture, but for those interested the Metasploit team has a really good whitepaper.

Command and Control

- Term used to define when an attack has “hands on keyboard access”.
- Attacker creates a command and control channel in order to continue to operate targets.
- This step is relatively generic and relevant throughout the attack, not only when malware is installed
- At this point the system is fully compromised.

Further Reading.



Stage 4: Persistence

- Now that we have access, lets keep it!
  - Malicious services
  - Service misconfigurations
  - Adding backdoors
  - Malicious user accounts.
  - Binary Shimming
  - Path Attacks

MITRE ATT&CK, PTES

Stage 5: Privilege Escalation

- Act of exploiting a bug, design flaw, or misconfiguration in an operating system or application to gain elevated access to resources that are normally protected.
- At this stage we want to get the highest level of privileges possible on a system.
  - Linux: root
  - Windows: SYSTEM/NT Auth
- This might occur before or in parallel with Stage 4
- Common Methods:
  - Credential Stealing
  - Service Elevation
  - System Kernel Modules

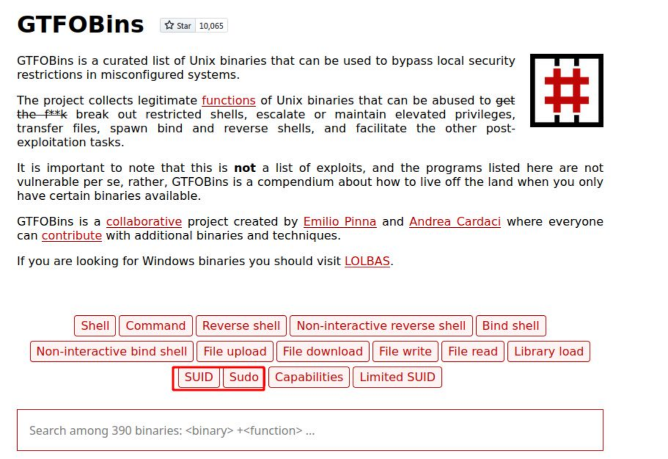
MITRE ATT&CK

Linux - Kernel Exploits

- The kernel is the main component of Linux operating system
- A linux kernel can be vulnerable to a bug that can be leveraged to escalate privileges
  - `uname -a`
- Workflow
  - Check the kernel version
  - Check if there is an exploit for the specific version
- https://github.com/Notselwyn/CVE-2024-1086

Linux - SUID Binaries

- SUID is a type of permission which is given to a file and allows users to execute the file with the permissions of the owner
- To search for SUID binaries
  - `find / -perm -u=s -type f 2>/dev/null`
- Look up these binaries on GTFObins (https://gtfobins.github.io)



GTFOBins

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

The project collects legitimate functions of Unix binaries that can be abused to ~~get the f**k~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

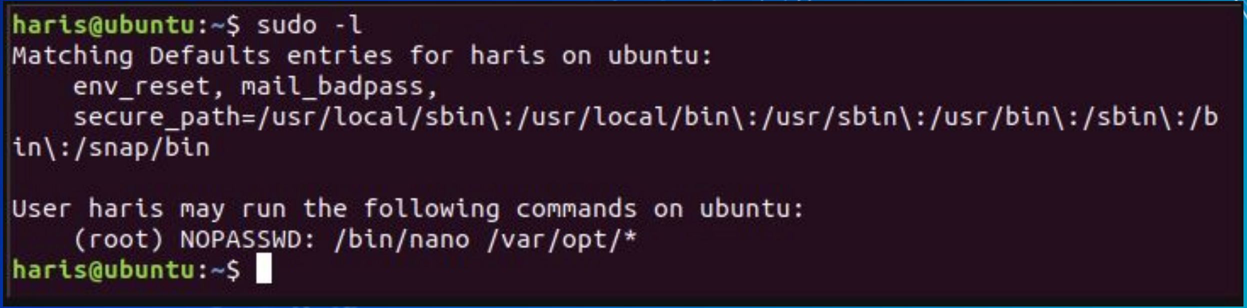
It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

GTFOBins is a collaborative project created by Emilio Pinna and Andrea Cardaci where everyone can contribute with additional binaries and techniques.

If you are looking for Windows binaries you should visit LOLBAS.

Linux - sudo permissions

- Sudo is “program for Unix-like computer operating systems that allows users to run programs with the security privileges of another user”
  - Selective sudo permissions are dangerous!
- `sudo -l`
- In this case, nano can be run with sudo permissions
  - How can we use this?



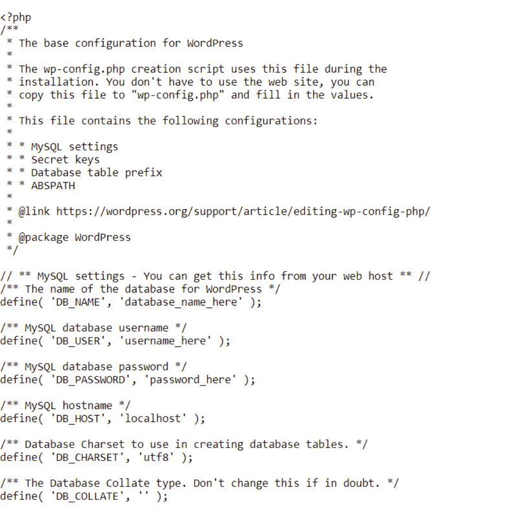
```
haris@ubuntu:~$ sudo -l
Matching Defaults entries for haris on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/b
in\:/snap/bin

User haris may run the following commands on ubuntu:
    (root) NOPASSWD: /bin/nano /var/opt/*
haris@ubuntu:~$ 
```

Linux - World Writable Files

- Writable Service Files
  - If any ".service" files are writable, you could modify it to run a reverse shell or other backdoor when a service is stopped, restarted, or started.
- Writable Service Binaries
  - The same logic applies with the service files, if you can write to an executable that is being ran as a service you can have a revershell or backdoor be triggered as the service user

Linux - Readable files

- Depending on the user you are currently running as it may be possible to read certain configuration files
  - find / -perm -o=r -type f 2>/dev/null (Will show alot of stuff beware!)
- These often contain credentials/keys which may be reused
- Be sure to check for files that look like the following:
  - config.* (config.php, config.json, config.xml, etc)
  - database .* (database.php, database.js, etc)
  - *.conf (mysql.conf, httpd.conf, etc)
  - id_dsa
  - id_rsa



```php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/support/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'database_name_here' );

/** MySQL database username */
define( 'DB_USER', 'username_here' );

/** MySQL database password */
define( 'DB_PASSWORD', 'password_here' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

Automated Tools:

- LinPEAS
  - https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/
- LinEnum
  - https://github.com/rebootuser/LinEnum
- LSE
  - https://github.com/diego-treitos/linux-smart-enumeration
- LinuxPrivChecker
  - https://github.com/sleventyeleven/linuxprivchecker

Demo

My friend Graham Edwards's company recently had some contractors build a filestore and sharing service for him. He doesn't really trust them so he asked me to see if I noticed anything about it and he'll buy me dinner next time he's in town.

The tool (called FileStorm) is located at filestorm.futuretools.us Because it's already been integrated into the rest of the infrastructure he doesn't want me to touch any other device on the network.

Windows Privilege Escalation

- Windows privilege escalation is a bit messy. [1], [2]
- Two levels:
  - Admin to SYSTEM
    - Relatively Easy
  - User to Admin
    - Lots of automated tooling.
    - WINpeas:
      - https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/winPEAS
    - JAWS:
      - https://github.com/411Hall/JAWS
- Active Directory adds another layer [1], [2]
  - http://howtopassoscp.com/
  - https://lolbas-project.github.io/#

Stage 6: Post Exploitation

- Pivoting [1] and Lateral Movement [2]
  - Move to another device or account.
  - Weak Credentials
  - Password Spraying
  - Hash Cracking (Kerberoasting, AS-REP Roasting)
  - Pass-the-Hash (SMB, WMI, Kerberos)
  - SSH Keys
  - Tunneling/proxying
  - Scan for new hosts/services
- Collection [3] and Exfiltration [4]
  - Harvest/Steal SPII or corporate data.
- PTES

All of this is scope dependant!

Don't commit crimes.

Federal Prison is bad.

Artifact Cleanup

- Leave the environment in the same state you found it
  - Remove persistence
  - Kill all shells
  - Any files you created are removed
    - Try to never create files
  - Safely destroy any client data you mate have obtained to ensure no leaking of private data of your client
  - Basically, any changes made must be reversed

Stage 7: Impact and Reporting

- Impact: disrupt availability or compromise integrity by manipulating business and operational processes
    - How much could you have affected business operations?
    - Data Destruction, Process Corruption
- Reporting = aka the $20,000 paper
    - Most important part of your job.
    - Explain what you've found, how you found it, why it's important, how to fix it.
    - Be professional.
        - Don't call the security team a "group of 18th century baboons"
    - Keep confidential data confidential.
        - Redact liberally.
    - It's about the client. Help the client.
        - Tailor your advice to their business needs.

Reporting cont..

Report Structure

1. Executive summary
   a. Deliverable for high level executives (NON TECHNICAL) to show business impact ($$$)
2. Project Overview & Methodology
3. Findings Summary & Remediation Summary
4. Findings
   a. Description: What is the vulnerability?
   b. Impact: What is the impact of this vulnerability?
   c. Remediation: How can the client fix this?
   d. Discovery: How was the vulnerability found?

Reporting cont..

- What remediation isn't:
  - “Just upgrade version”
  - “Just patch it”
  - “simply turn it off”
- Usually it is NOT that simple
  - We only see snapshot of business infra and processes
  - Don't assume clients infrastructure
    - Legacy services
    - Budget, personnel, time
- Provide multiple potential remediations with detail
  - Learned insights from being a builder + defender

Demo

My friend Graham Edwards's company recently had some contractors build a filestore and sharing service for him. He doesn't really trust them so he asked me to see if I noticed anything about it and he'll buy me dinner next time he's in town.

The tool (called FileStorm) is located at filestorm.futuretools.us Because it's already been integrated into the rest of the infrastructure he doesn't want me to touch any other device on the network.

Hands On

UBNetDef is developing a multi role chatops server in preparation for an upcoming competition. The only problem was that some of the developers ran out of redbull half way through the project so it’s probably not secure as it should be.

They’ve asked you to use your skills from the Pentesting lecture to identify and exploit **at least one** method of gaining initial access to the system.

The system is located at ??? on your ServerNet network.

Homework

Based on the flaws discover in the in class VM, UBNetDef CISO Kevin Cleary has decided that all current UBNetDef projects must undergo a vulnerability assessment.

He’s deployed copies of the new distributed computing server somewhere on your ServerNet and asks your provide a full report on vulnerabilities and remediation.

You will be graded on the quality of your submission, not on the quantity of vulnerabilities found.

Please start early. This is a tough one.